AURASCAPE SHIFTS CONTAINER SECURITY LEFT

CASE STUDY

CUSTOMER SNAPSHOT

COMPANY
Aurascape

INDUSTRY
AI Security

ARCHITECTURE
Cloud-native, Kubernetes-based platform

Aurascape builds security solutions for the AI era on a modern, cloud-native platform where confidence in the software foundation is critical. As the platform scaled, the team recognized the importance of establishing security assurances earlier in the build lifecycle.

"Standardizing on verified container foundations gave us confidence in the base of every service we deploy and allowed us to shift security much earlier in the build process."

Mr. Moinul Khan
CEO, AURASCAPE

CONTEXT AND OBJECTIVE

Aurascape's platform spans multiple execution environments and technologies. This architectural flexibility enabled rapid innovation, but it also introduced variation in how container images were built, packaged, and validated.

To support continued growth without compromising confidence, Aurascape made a deliberate decision to standardize container foundations across the platform and move assurance as early as possible into the build process. Rather than relying primarily on downstream scanning and point-in-time checks, the goal was to ensure that every service started from a trusted, repeatable, and verifiable base.

WHY EARLY ASSURANCE MATTERS

Security and compliance questions often surface late in the lifecycle, during production readiness reviews, audit cycles, or deployment approvals. While container scanning remained part of Aurascape's workflow, it typically occurred after images were already built, pushing potential issues downstream.

Aurascape wanted stronger guarantees earlier in the pipeline, focusing on:

Consistent
Consistent across environments

Explainable
Explainable from a dependency standpoint

Verifiable
Cryptographically verifiable metadata

"This approach was guided by a simple principle: trust should be built into the process, not inferred after the fact."

ESTABLISHING A CONSISTENT FOUNDATION

Operating across multiple teams and environments naturally introduces variability in how software is built. Aurascape addressed this by applying a unified trust model at the base image layer, with an emphasis on:

- Standardized foundations across services and teams
- Predictable build behavior to reduce drift and configuration variance
- Transparent provenance and dependencies to support faster reviews and compliance checks

This standardized baseline became increasingly important as the platform expanded in scope and scale.

THE CLEANSTART APPROACH

To put this model into practice, Aurascape adopted **CleanStart images** as the standardized foundation layer for its platform.

CleanStart images are built from source using deterministic, hermetic pipelines, enabling Aurascape to:

- ✓ Establish a verifiable, standardized container baseline across all services
- ✓ Gain full visibility into all dependencies and apply consistent security controls
- ✓ Generate standardized SBOMs and cryptographically verifiable provenance

By integrating CleanStart early in the build process, Aurascape embedded security and transparency into the platform foundation before application code was introduced.

OUTCOMES

A more consistent security posture across services

Fewer vulnerabilities at image release, reducing downstream remediation

Faster onboarding of new services using pre-verified image foundations

Improved audit readiness through standardized SBOMs and build evidence

WHY THIS MATTERS

Aurascape's experience shows that strong security outcomes start with intentional foundations. By prioritizing early assurance, standardized builds, and verifiable provenance, the company aligned its internal engineering practices with the same trust principles it delivers to customers.